JOURNAL OF NUMBER THEORY 22, 249–270 (1986)

Binäre quadratische Formen und rationale Zerlegungsgesetze I

FRANZ HALTER-KOCH

Mathematisches Institut, Universität Graz, Halbärthgasse 1/1, A-8010 Graz, Austria

Communicated by P. Roquette

Received January 23, 1984

HERRN PROF. DR. A. AIGNER ZUM 75. GEBURTSTAG

1. EINLEITUNG

Eines der zentralen Probleme der algebraischen Zahlentheorie ist die Frage nach rationalen Zerlegungsgesetzen: Für einen Zahlkörper K und eine rationale Primzahl p ist durch rational formulierbare (von den Daten von K abhängige) Kriterien zu entscheiden, wie sich p in K zerlegt. Dieses Problem ist für abelsche Zahlköper vollständig gelöst: Ist nämlich $K/\mathbb{Q}$ abelsch und m der Führer von $K/\mathbb{Q}$ (das ist die kleinste natürliche Zahl f, für die K im Körper der f-ten Einheitswurzeln enthalten ist), so hängt das Zerlegungsverhalten einer rationalen Primzahl p mit $p \nmid m$ nur von der Ordnung der Restklasse $p \bmod m$ ab. Ist Ω ein quadratischer Zahlkörper mit Diskriminante d und K ein Ringklassenkörper über Ω, so hat man für den Körper K ebenfalls ein rationales Zerlegungsgesetz: Ist f der Führer von K/Ω, so ist K/Ω Klassenkörper zu einer Untergruppe der vollen Ringklassengruppe $\bmod f$ in Ω, und diese ist (in explizit angebbarer Weise) isomorph zur Kompositionsklassengruppe der ganzzahligen binären quadratischen Formen der Diskriminante df^2; auf Grund dieses Zusammenhanges ist das Zerlegungsverhalten einer rationalen Primzahl p mit $p \nmid df$ in K beschreibbar durch die Darstellbarkeit von p bzw. p^2 durch gewisse Klassen binärer quadratischer Formen der Diskriminante df^2. Der Begriff des Ringklassenkörpers wurde von P. Satge [18] weitgehend verallgemeinert: Sei L ein galoisscher algebraischer Zahlkörper und $\mathbb{Q} \subset K \subset L$ derart, daß $K/\mathbb{Q}$ galoissch, L/K abelsch und die Verlagerung von $\mathbb{Q}$ nach K trivial ist; ferner sei $[L: K]$ ungerade, falls K reell und $[K: \mathbb{Q}] > 2$ ist; dann kann man das Zerlegungsverhalten von p in L beschreiben durch die Darstellbarkeit von Potenzen p^r $(r \leqslant [K: \mathbb{Q}])$ durch gewisse zu K gehörige Normformen.

Die Frage nach rationalen Zerlegungsgesetzen ist eng verbunden mit der Frage nach rationalen Potenzrestkriterien: Nach welchen Primzahlen p ist

0022-314X/86 $3.00

eine (ganzrationale oder geeignete ganzalgebraische) Zahl α ein m-ter Potenzrest? Das ist nämlich sicher (und in den meisten interessierenden Fällen auch nur) dann der Fall, wenn p im Körper $\mathbb{Q}(\xi_m, \sqrt[m]{\alpha})$ voll zerfällt (ξ_m ist eine primitive m-te Einheitswurzel). Im Gegensatz zur eingangs gestellten Frage nach rationalen Kriterien zur Bestimmung des Zerlegungsverhaltens einer rationalen Primzahl wird hier nur noch die schwächere Frage nach Kriterien für den vollen Zerfall gestellt. Einen Überblick über rationale Potenzrestkriterien, welche durch solche "schwache Zerlegungsgesetze" gewonnen wurden, findet man in [4] (siehe auch [5, 6]).

P. Barrucand und H. Cohn [3] bewiesen das folgende Kriterium für eine Primzahl $p = x^2 + 8y^2$: y ist gerade oder ungerade, je nachdem, ob $1 + \sqrt{2}$ quadratischer Rest oder Nichtrest mod p ist. Dieses Ergebnis kann man auch als Kriterium dafür interpretieren, welche der beiden Klassen in Hauptgeschlecht binärer quadratischer Formen der Diskriminante -2^7 die Primzahl p darstellt. Im Anschluß an diese Arbeit entwickelte sich ein lebhaftes Interesse an expliziten Potenzrestkriterien für Grundeinheiten reell-quadratischer Zahlkörper (siehe [15, 16, 7] und die dort zitierte Literatur). Ein systematischer Zusammenhang zwischen einigen dieser Kriterien (vor allem für quadratische und biquadratische Reste) und schwachen rationalen Zerlegungsgesetzen wurde erstmals in [14] und [10] hergestellt.

Es gibt aber auch eine Reihe rationaler Potenzrestkriterien, welche nicht mit der Methode der schwachen Zerlegungsgesetze, sondern direkt mit Hilfe Jacobi'scher Summen gewonnen wurden (siehe [20, 21, 17, 15, 7]). Obwohl einige dieser Kriterien auch mit Hilfe von Zerlegungsgesetzen bewiesen werden konnten (siehe [1, 8]), scheint es doch so zu sein, daß die Methode der direkten Berechnung Jacobi'scher Summen—sofern sie anwendbar ist—der Methode der expliziten Zerlegungsgesetze überlegen ist. Die in Rede stehenden Kriterien sind von dem Typ, daß sich eine Primzahl p durch zwei quadratische Formen darstellen läßt und zwischen diesen beiden Darstellungen Kongruenzbedingungen bestehen. Von diesem Typ sind auch die von E. Lehmer [15] vermuteten und bisher unbewiesenen Kriterien zum 4. Potenzcharakter der Grundeinheiten von $\mathbb{Q}(\sqrt{q})$ ($q = 5$, 13, 37) und zum 8. Potenzcharakter der Grundeinheit von $\mathbb{Q}(\sqrt{7})$; ein entsprechendes Kriterium für den 8. Potenzcharakter von $2 + \sqrt{3}$ wurde in [7] mit expliziten Jacobi'schen Summen der Ordnung 12 bewiesen, eine Anwendung der Methode auf $\mathbb{Q}(\sqrt{7})$ würde die Kenntnis Jacobi'scher Summen der Ordnung 28 erforderlich machen.

In der vorliegenden Arbeit leite ich schwache rationale Zerlegungsgesetze (welche die voll zerfallenden Primzahlen kennzeichnen) vom Typ "Darstellung durch binäre quadratische Formen mit Kongruenzbedingungen" für folgende Körper $\tilde{K}$ her: $\tilde{K}$ ist der volle Strahlklassenkör-

per modulo 2^t ($t \geqslant 2$) über einem biquadratisch-bizyklischen Zahlkörper $K = \mathbb{Q}(\sqrt{q}, \sqrt{d})$ ($q \equiv 5 \bmod 8$, $d \equiv -1 \bmod 8$, $\mathbb{Q}(\sqrt{d})$ enthält eine Einheit $\eta \equiv \sqrt{d} \bmod 2$) oder ein geeigneter Teilkörper desselben. Dazu betrachte ich zunächst quadratische Zahlkörper $\Omega = \mathbb{Q}(\sqrt{\Delta})$ und zeige, wie man für Strahlklassenkörper modulo 2^t über Ω schwache Zerlegungsgesetze herleiten kann; dazu genügt es, in Ω zerlegte Primzahlen $p \neq 2$ zu betrachten und ein rationales Kriterium dafür anzugeben, daß p in Ω einen Primteiler π mit vorgegebener Restklasse mod 2^t (vorzugsweise $\pi \equiv 1 \bmod 2^t$) hat. Die Resultate im biquadratisch-bizyklischen Fall entstehen dann durch Betrachtung der Normen in Bezug auf die quadratischen Teilkörper und Zusammensetzen der Resultate aus dem quadratischen Fall.

In manchen Fällen kann man für die Strahlklassenkörper modulo 2^t über $\mathbb{Q}(\sqrt{q}, \sqrt{-1})$ Radikalerzeugungen angeben und erhält rationale Potenzrestkriterien für die Radikanden. So erhält man dann beispielsweise die bisher unbewiesenen Kriterien aus [15], aber auch viele andere.

Ähnliche Überlegungen sind für alle biquadratisch-bizyklischen Körper, in denen 2 nicht voll zerfällt, durchführbar. Ich werde in einer nachfolgenden Arbeit darauf eingehen.

2. Quadratische Zahlkörper

Sei $\Delta \in \mathbb{Z}$ quadratfrei, $\alpha \in \mathbb{Q}(\sqrt{\Delta})$ ganz und prim zu 2; dann hat man eine Darstellung $N(\alpha) = x^2 - \Delta y^2$,[1] und ich untersuche, wie sich die Restklasse von $\alpha \bmod 2^t$ in x und y widerspiegelt. Die Aussagen dieses Paragraphen sind (von einigen Zusätzen abgesehen) leicht zu beweisen und wohl auch teilweise bekannt. Die nachfolgenden Anwendungen scheinen mir jedoch eine ausführliche Darstellung zu rechfertigen.

Sei im folgenden $t \geqslant 2$; die Basiselemente für die primen Restklassengruppen und deren Ordnungen mod 2^t entnehme ich aus [9].

a. $\Delta \equiv -1 \bmod 8$

Sei $\delta \in \mathbb{Z}[\sqrt{\Delta}]$ eine primitive 4. Einheitswurzel mod 2^{t+1}, also insbesondere $\delta \equiv \sqrt{\Delta} \bmod 2$. Dann hat jedes zu 2 prime $\alpha \in \mathbb{Z}[\sqrt{\Delta}]$ eine Darstellung

$$\alpha = \delta^A \cdot 5^B \cdot (-1 + 2\sqrt{\Delta})^C + 2^t \gamma_0 \tag{1}$$

mit $A, B, C \geqslant 0$ und $\gamma_0 = u_0 + v_0\sqrt{\Delta} \in \mathbb{Z}[\sqrt{\Delta}]$; dabei ist $A \bmod 4$, $B \bmod 2^{t-2}$ und $C \bmod 2^{t-1}$ eindeutig bestimmt.

[1] N ist in diesem Abschnitt die Norm für $\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}$.

Schreibt man $\alpha = X + Y\sqrt{\Delta}$ mit $X, Y \in \mathbb{Z}$, so folgt wegen $\alpha \equiv \delta^A \bmod 2$:

In (1) *ist genau dann* $A \equiv 0 \bmod 2$, *wenn* $N(\alpha) = X^2 - 4\Delta Y^2$ *mit* $X, Y \in \mathbb{Z}$; *im Falle* $A \equiv 1 \bmod 2$ *ist* $N(\alpha) = 4X^2 - \Delta Y^2$ *mit* $X, Y \in \mathbb{Z}$.

Sei nun $\alpha \in \mathbb{Z}[\sqrt{\Delta}]$ prim zu 2 und in der Darstellung (1) mit $A \equiv 0 \bmod 2$ gegeben (also $\alpha \equiv 1 \bmod 2$). Ich setze $C = 2^c \cdot C_0$ mit $c \geqslant 0$ und $C_0 \equiv 1 \bmod 2$, falls $c < t$. Dann ist

$$(-1 + 2\sqrt{\Delta})^C \equiv 1 + 2C + 2C\sqrt{\Delta} \bmod 2^{c+2},$$

also

$$\alpha \equiv \pm 5^B \cdot (1 + 2C + 2C\sqrt{\Delta} + 2^{c+2}\gamma_1) + 2^t\gamma_0 \bmod 2^{t+1}$$

mit $\gamma_1 = u_1 + v_1\sqrt{\Delta} \in \mathbb{Z}[\sqrt{\Delta}]$. Hiermit erhalte ich

$$N(\alpha) = X_0^2 - \Delta Y_0^2$$

mit

$$X_0 \equiv 5^B \cdot (1 + 2C + 2^{c+2}u_1) + 2^t u_0 \bmod 2^{t+1},$$
$$Y_0 \equiv 5^B \cdot (2C + 2^{c+2}v_1) + 2^t v_0 \bmod 2^{t+1};$$

daraus folgt

für	$0 \leqslant c < t-1$:	$X_0 \equiv 5^B + 2^{c+1}$,	$Y_0 \equiv 2^{c+1} \bmod 2^{c+2}$;
für	$c = t-1$:	$X_0 \equiv 5^B + 2^t(1+u_0)$,	$Y_0 \equiv 2^t \cdot (1+v_0) \bmod 2^{t+1}$;
für	$c \geqslant t$:	$X_0 \equiv 5^B + 2^t u_0$,	$Y_0 \equiv 2^t v_0 \bmod 2^{t+1}$.

Insbesondere habe ich damit bewiesen:

Ist $\alpha \in \mathbb{Z}[\sqrt{\Delta}]$ *prim zu* 2 *und in der Darstellung* (1) *gegeben, so ist genau dann* $A \equiv 0 \bmod 2$, $B \equiv 0 \bmod 2^{t-2}$ *und* $C \equiv 0 \bmod 2^{t-1}$ (*also* $\alpha \equiv \pm 1 \bmod 2^t$), *wenn* $N(\alpha) = X^2 - 4^t\Delta Y^2$ *mit* $X, Y \in \mathbb{Z}$ *und* $X \equiv 1 \bmod 2^t$. *Dabei ist*

$$Y \equiv \begin{cases} 1 + v_0 \bmod 2 & \text{falls } C \not\equiv 0 \bmod 2^t, \\ v_0 \bmod 2 & \text{falls } C \equiv 0 \bmod 2^t. \end{cases}$$

b. $\Delta \equiv 3 \bmod 8$

Jedes zu 2 prime $\alpha \in \mathbb{Z}[\sqrt{\Delta}]$ hat eine Darstellung

$$\alpha = \pm\sqrt{\Delta}^B \cdot (-1 + 2\sqrt{\Delta})^C + 2^t\gamma_0 \tag{2}$$

mit $B, C \geqslant 0$ und $\gamma_0 = u_0 + v_0\sqrt{\Delta} \in \mathbb{Z}[\sqrt{\Delta}]$; dabei sind B und C mod 2^{t-1} eindeutig bestimmt.

Schreibt man $\alpha = X + Y\sqrt{\Delta}$ mit $X, Y \in \mathbb{Z}$, so folgt wegen $\alpha \equiv \sqrt{\Delta}^B \bmod 2$:

In (2) *ist genau dann* $B \equiv 0 \bmod 2$, *wenn* $N(\alpha) = X^2 - 4\Delta Y^2$ *mit* $X, Y \in \mathbb{Z}$; *im Falle* $B \equiv 1 \bmod 2$ *ist* $N(\alpha) = 4X^2 - \Delta Y^2$ *mit* $X, Y \in \mathbb{Z}$.

Sei nun $\alpha \in \mathbb{Z}[\sqrt{\Delta}]$ prim zu 2 und in der Darstellung (2) mit $B \equiv 0 \bmod 2$ gegeben (also $\alpha \equiv 1 \bmod 2$). Ich setze $B = 2B'$ und $C = 2^c C_0$ mit $c \geqslant 0$ und $C_0 \equiv 1 \bmod 2$, falls $c < t$. Wegen

$$(-1 + 2\sqrt{\Delta})^C \equiv 1 + 2C + 2C\sqrt{\Delta} \bmod 2^{c+2}$$

ist

$$\alpha = \pm \Delta^{B'} \cdot (1 + 2C + 2C\sqrt{\Delta} + 2^{c+2}\gamma_1) + 2^t\gamma_0$$

mit $\gamma_1 = u_1 + v_1\sqrt{\Delta} \in \mathbb{Z}[\sqrt{\Delta}]$, und ich erhalte

$$N(\alpha) = X_0^2 - \Delta Y_0^2,$$

wobei

$$X_0 = \Delta^{B'} \cdot (1 + 2C + 2^{c+2}u_1) + 2^t u_0,$$
$$Y_0 = \Delta^{B'} \cdot (2C + 2^{c-2}v_1) + 2^t v_0;$$

daraus folgt

für	$0 \leqslant c < t-1$:	$X_0 \equiv \Delta^{B'} + 2^{c+1}$,	$Y_0 \equiv 2^{c+1} \bmod 2^{c+2}$;
für	$c = t-1$:	$X_0 \equiv \Delta^{B'} + 2^t \cdot (1 + u_0)$,	$Y_0 \equiv 2^t \cdot (1 + v_0) \bmod 2^{t+1}$;
für	$c \geqslant t$:	$X_0 \equiv \Delta^{B'} + 2^t u_0$,	$Y_0 \equiv 2^t v_0 \bmod 2^{t+1}$.

Insbesondere habe ich damit bewiesen:

Ist $\alpha \in \mathbb{Z}[\sqrt{\Delta}]$ *prim zu* 2 *und in der Darstellung* (2) *gegeben, so ist genau dann* $B \equiv C \equiv 0 \bmod 2^{t-1}$ (*also* $\alpha \equiv \pm 1 \bmod 2^t$), *wenn* $N(\alpha) = X^2 - 4^t \Delta Y^2$ *mit* $X, Y \in \mathbb{Z}$ *und* $X \equiv 1 \bmod 2^t$. *Dabei ist*

$$Y \equiv \begin{cases} 1 + v_0 \bmod 2 & \text{falls } C \not\equiv 0 \bmod 2^t, \\ v_0 \bmod 2 & \text{falls } C \equiv 0 \bmod 2^t. \end{cases}$$

c. $\Delta \equiv 5 \bmod 8$.

Sei $\omega \in \mathbb{Z}[(1 + \sqrt{\Delta})/2]$ eine primitive 3. Einheitswurzel mod 2^{t+1}. Dann hat jedes zu 2 prime $\alpha \in \mathbb{Z}[(1 + \sqrt{\Delta})/2]$ eine Darstellung

$$\alpha = \pm \omega^A \cdot \sqrt{\Delta}^B \cdot (-1 + 2\sqrt{\Delta})^C + 2^t\gamma_0 \tag{3}$$

mit $A, B, C \geq 0$ und $\gamma_0 = \frac{1}{2} \cdot (u_0 + v_0 \sqrt{\Delta}) \in \mathbb{Z}[(1+\sqrt{\Delta})/2]$, d.h. $u_0, v_0 \in \mathbb{Z}$, $u_0 \equiv v_0 \bmod 2$; dabei ist $A \bmod 3$, $B \bmod 2^{t-1}$ und $C \bmod 2^{t-2}$ eindeutig bestimmt.

Schreibt man $\alpha = \frac{1}{2} \cdot (X + Y\sqrt{\Delta})$ mit $X, Y \in \mathbb{Z}$, so folgt wegen $\alpha \equiv \omega^A \cdot \sqrt{\Delta}^B \bmod 4$:

In (3) *ist genau dann* $A \equiv 0 \bmod 3$, *wenn* $N(\alpha) = X_0^2 - \Delta Y_0^2$ *mit* $X_0, Y_0 \in \mathbb{Z}$; *andernfalls ist* $4N(\alpha) = X^2 - \Delta Y^2$ *mit* $X, Y, \in \mathbb{Z}$, $X \equiv Y \equiv 1 \bmod 2$. *Ist* $A \equiv 0 \bmod 3$, *so ist genau dann* $B \equiv 0 \bmod 2$, *wenn* $N(\alpha) = X^2 - 4\Delta Y^2$ *mit* $X, Y \in \mathbb{Z}$; *im Falle* $B \equiv 1 \bmod 2$ *ist* $N(\alpha) = 4X^2 - \Delta Y^2$ *mit* $X, Y \in \mathbb{Z}$.

Sei nun $\alpha \in \mathbb{Z}[(1+\sqrt{\Delta})/2]$ prim zu 2 und in der Darstellung (3) mit $A \equiv 0 \bmod 3$ und $B \equiv 0 \bmod 2$ gegeben; dann ist $\alpha \in \mathbb{Z}[\sqrt{\Delta}]$, $\alpha \equiv 1 \bmod 4$, und ich setze $B = 2B'$, $C = 2^c C_0$ mit $c \geq 0$ und $C_0 \equiv 1 \bmod 2$, falls $c < t-1$. Wegen

$$(-1 + 2\sqrt{\Delta})^C \equiv 1 + 2C + 2C\sqrt{\Delta} \bmod 2^{c+2}$$

ist

$$\alpha \equiv \pm \Delta^{B'} \cdot (1 + 2C + 2C\sqrt{\Delta} + 2^{c+2}\gamma_1) + 2^t \gamma_0 \bmod 2^{t+1}$$

mit $\gamma_1 = \frac{1}{2}(u_1 + v_1\sqrt{\Delta}) \in \mathbb{Z}[(1+\sqrt{\Delta})/2]$, d.h., $u_1, v_1 \in \mathbb{Z}$, $u_1 \equiv v_1 \bmod 2$, und ich erhalte

$$N(\alpha) = X_0^2 - \Delta Y_0^2$$

mit

$$X_0 \equiv \Delta^{B'} \cdot (1 + 2C + 2^{c+1}u_1) + 2^{t-1}u_0 \bmod 2^t,$$
$$Y_0 \equiv \Delta^{B'} \cdot (2C + 2^{c+1}v_1) + 2^{t-1}v_0 \bmod 2^t;$$

daraus folgt

$$\text{für } 0 \leq c < t-1: \quad X_0 \equiv \Delta^{B'}, \qquad Y_0 \equiv 0 \bmod 2^{c+1};$$
$$\text{für } c \geq t-1: \quad X_0 \equiv \Delta^{B'} + 2^{t-1}u_0, \quad Y_0 \equiv 2^{t-1}v_0 \bmod 2^t.$$

Damit ist (unter Beachtung von $u_0 \equiv v_0 \bmod 2$) insbesondere bewiesen:

Ist $\alpha \in \mathbb{Z}[(1+\sqrt{\Delta})/2]$ *prim zu* 2 *und in der Darstellung* (3) *gegeben, so ist genau dann* $A \equiv 0 \bmod 3$, $B \equiv 0 \bmod 2^{t-1}$ *und* $C \equiv 0 \bmod 2^{t-2}$ (*also* $\alpha \equiv \pm 1 \bmod 2^t$), *wenn* $N(\alpha) = X^2 - 4^{t-1}\Delta Y^2$ *mit* $X, Y \in \mathbb{Z}$ *und* $X \equiv 1 + 2^{t-1}Y \bmod 2^t$; *dabei ist* $Y \equiv v_0 \bmod 2$.

d. $\Delta \equiv 2 \bmod 4$

Jedes zu 2 prime $\alpha \in \mathbb{Z}[\sqrt{\Delta}]$ hat eine Darstellung

$$\alpha = \pm 5^B \cdot (1 + \sqrt{\Delta})^C + 2^t \gamma_0 \tag{4}$$

mit $B \geqslant 0$, $C \geqslant 1$ und $\gamma_0 = u_0 + v_0 \sqrt{\Delta} \in \mathbb{Z}[\sqrt{\Delta}]$; dabei ist $B \bmod 2^{t-2}$ und $C \bmod 2^t$ eindeutig bestimmt. Ich setze $C = 2^c \cdot C_0$ mit $c \geqslant 0$ und $C_0 \equiv 1 \bmod 2$, falls $c \leqslant t$. Wegen

$$(1 + \sqrt{\Delta})^C \equiv \pm 1 + C\sqrt{\Delta} \bmod 2^{c+1}$$

folgt

$$\alpha = \pm 5^B \cdot (1 + C\sqrt{\Delta} + 2^{c+1}\gamma_1) + 2^t\gamma_0$$

mit $\gamma_1 = u_1 + v_1\sqrt{\Delta} \in \mathbb{Z}[\sqrt{\Delta}]$, und ich erhalte

$$N(\alpha) = X_0^2 - \Delta Y_0^2$$

mit

$$X_0 = 5^B \cdot (1 + 2^{c+1}u_1) + 2^t u_0,$$
$$Y_0 = 5^B \cdot (C + 2^{c+1}v_1) + 2^t v_0;$$

daraus folgt

$$\begin{array}{lll} \text{für } 0 \leqslant c < t: & X_0 \equiv 5^B, & Y_0 \equiv 2^c \bmod 2^{c+1}; \\ \text{für } c = t: & X_0 \equiv 5^B + 2^t u_0, & Y_0 \equiv 2^t \cdot (1 + v_0) \bmod 2^{t+1}; \\ \text{für } c > t: & X_0 \equiv 5^B + 2^t u_0, & Y_0 \equiv 2^t v_0 \bmod 2^{t+1}. \end{array}$$

Damit ist insbesondere bewiesen:

Ist $\alpha \in \mathbb{Z}[\sqrt{\Delta}]$ prim zu 2 und in der Darstellung (4) gegeben, so ist genau dann $B \equiv 0 \bmod 2^{t-2}$ und $C \equiv 0 \bmod 2^t$ (also $\alpha \equiv \pm 1 \bmod 2^t$), wenn $N(\alpha) = X^2 - 4^t \Delta Y^2$ mit $X, Y \in \mathbb{Z}$ und $X \equiv 1 \bmod 2^t$. Dabei ist

$$Y \equiv \begin{cases} 1 + v_0 \bmod 2 & \text{falls } C \not\equiv 0 \bmod 2^{t+1}, \\ v_0 \bmod 2 & \text{falls } C \equiv 0 \bmod 2^{t+1}. \end{cases}$$

3. Biquadratische Körper $K = \mathbb{Q}(\sqrt{d}, \sqrt{q})$ mit $d \equiv -1$, $q \equiv 5 \bmod 8$

Seien $d, q \in \mathbb{Z}$ quadratfrei, $d \equiv -1 \bmod 8$, $q \equiv 5 \bmod 8$ und $K = \mathbb{Q}(\sqrt{d}, \sqrt{q})$ und $dq = m^2 q^*$ mit (ungeradem) $m \in \mathbb{N}$ und quadratfreiem $q^* \equiv 3 \bmod 8$. Dann ist $2 \cong \mathfrak{w}^2$ in K, $\mathfrak{w}$ hat Restklassengrad 2 und $\pi = 1 - \sqrt{d}$ ist ein Primelement für $\mathfrak{w}$ in der Komplettierung $K_{\mathfrak{w}}$. Ich bestimme nun zunächst eine Basis für die Einheitengruppe $U_{\mathfrak{w}}$ von $K_{\mathfrak{w}}$ und benutze diese dann zur Bescheibung der primen Restklassengruppen modulo 2^t in K.

Nach [11, chap. 15.6, IVbα], hat jede Einseinheit $\eta \in U_{\mathfrak{w}}^1 \subset U_{\mathfrak{w}}$ eine eindeutige Darstellung in der Form

$$\eta = \zeta^Q \cdot (1+\xi\pi)^A \cdot (1+\xi\pi^3)^B \cdot (1+\pi^3)^C \cdot (1+\xi\pi^4)^D$$

mit einer primitiven 4. Einheitswurzel $\zeta \in K_{\mathfrak{w}}$, $\xi = (-1+\sqrt{q})/2$ (Repräsentant einer primitiven 3. Einheitswurzel modulo $\mathfrak{w}$), $Q \in \mathbb{Z}/4\mathbb{Z}$ und $A, B, C, D \in \mathbb{Z}_2$. Die folgende Tabelle gibt die Ordnung der Basiselemente modulo $\mathfrak{w}^l$ ($l \geqslant 1$; negative Exponenten sind durch 0 zu ersetzen):

β	$1+\xi\pi$	$1+\xi\pi^3$	$1+\pi^3$	$1+\xi\pi^4$
$\mathrm{ord}_{\mathfrak{w}^l}(\beta)$	$2^{\{l/2\}+1}$	$2^{\{(l-1)/2\}}$	$2^{\{(l-1)/2\}}$	$2^{\{l/2\}-1}$

Dabei ist

$$\left\{\frac{k}{2}\right\} = \begin{cases} \dfrac{k}{2}-1 & \text{falls } k \text{ gerade,} \\ \dfrac{k-1}{2} & \text{falls } k \text{ ungerade.} \end{cases}$$

Als nächstes berechne ich die Normen der Basiselemente in bezug auf die quadratischen Teilkörper und stelle sie mit Hilfe der in 2. angegebenen Basiselemente mit Exponenten in $\mathbb{Z}_2$ dar. Ich schreibe im folgenden N_d, N_{q^*} und N_q für die Normen von $K/\mathbb{Q}(\sqrt{d})$, $K/\mathbb{Q}(\sqrt{q^*})$ und $K/\mathbb{Q}(\sqrt{q})$; dann gilt:

$$\begin{aligned} N_d(1+\xi\pi) &= \frac{1}{4}\cdot(1+d)(1-q) + \frac{1+q}{2}\sqrt{d} \\ &= \pm\delta \cdot 5^{b_1} \cdot (-1+2\sqrt{d})^{2c_1} \equiv \frac{1+q}{2}\sqrt{d} \bmod 8, \end{aligned}$$

$$\begin{aligned} N_d(1+\xi\pi^3) &= \frac{1-q}{4}\cdot\{(1+3d)^2 + d(3+d)^2\} - 3d \\ &\quad + \left\{\frac{1}{2}\cdot(1+3d)\cdot(3+d)\cdot(q-1) + 3 + d\right\}\sqrt{d} \\ &= 5^{b_2}\cdot(-1+2\sqrt{d})^{c_2} \equiv 3 + 2\sqrt{d} \bmod 8 \end{aligned}$$

mit $b_2 \equiv 1 \bmod 2$, $c_2 \equiv 1 \bmod 4$,

$$\begin{aligned} N_d(1+\pi^3) &= d^3 + 15d^2 + 21d + 4 - 2\cdot(3d^2+11d+6)\sqrt{d} \\ &= 5^{2b_3}\cdot(-1+2\sqrt{d})^{2c_3} \equiv 5 + 4\sqrt{d} \bmod 8 \end{aligned}$$

mit $c_3 \equiv 1 \bmod 2$,

$$N_d(1+\xi\pi^4) = \frac{1-q}{4}\cdot[16d(1+d)^2+(1+6d+d^2)^2]-6d-d^2+2(1+d)$$
$$\cdot[(1+6d+d^2)(1+q)-12d-2d^2]\cdot\sqrt{d}$$
$$= 5^{b_4}\cdot(-1+2\sqrt{d})^{4c_4} \equiv 5 \bmod 8$$

mit $b_4 \equiv 1 \bmod 2$,

$$N_{q^*}(1+\xi\pi) = \tfrac{1}{4}\cdot(1-d)(1-q)-m\cdot\sqrt{q^*}$$
$$= \sqrt{q^*}^{e_1}\cdot(-1+2\sqrt{q^*})^{f_1} \equiv 2 \pm \sqrt{q^*} \bmod 4$$

mit $e_1 \equiv f_1 \equiv 1 \bmod 2$,

$$N_{q^*}(1+\xi\pi^3) = -3d+\frac{1}{4}\cdot(1-d)^3(1-q)-(3+d)\,m\sqrt{q^*}$$
$$= \sqrt{q^*}^{2e_2}\cdot(-1+2\sqrt{q^*})^{f_2} \equiv -1+2\sqrt{q^*} \bmod 4$$

mit $f_2 \equiv 1 \bmod 2$,

$$N_{q^*}(1+\pi^3) = (4-d)\cdot(1+d+d^2)$$
$$= \sqrt{q^*}^{2e_3}\cdot(-1+2\sqrt{q^*})^{4f_3} \equiv 5 \bmod 8$$

mit $e_3 \equiv 1 \bmod 2$,

$$N_{q^*}(1+\xi\pi^4)$$
$$= \frac{1-q}{4}\cdot[(1+6d+d^2)^2-16d(1+d)^2]-6d-d^2-4(1+d)\,m\sqrt{q^*}$$
$$= \sqrt{q^*}^{2e_4}\cdot(-1+2\sqrt{q^*})^{4f_4} \equiv 5 \bmod 8$$

mit $e_4 \equiv 1 \bmod 2$,

$$N_q(1+\xi\pi) = \frac{1}{4}\cdot(1-d)(1+q)+\frac{1+d}{2}\sqrt{q}$$
$$= \pm\sqrt{q}^{2g_1}\cdot(-1+2\sqrt{q})^{h_1} \equiv 3 \bmod 4,$$
$$N_q(1+\xi\pi^3) = \frac{1}{4}\cdot(1-d)^3(1+q)-3d+\left\{1+3d+\frac{(d-1)^3}{2}\right\}\sqrt{q}$$
$$= \pm\sqrt{q}^{4g_2}\cdot(-1+2\sqrt{q})^{h_2} \equiv 5+2\sqrt{q} \bmod 8$$

mit $h_2 \equiv 1 \bmod 2$,

$$N_q(1+\pi^3) = (1-d)^3 + 3\cdot(1+2d)$$
$$= \sqrt{q}^{2g_3}\cdot(-1+2\sqrt{d})^{2h_3} \equiv 5 \bmod 8$$

mit $g_3 \equiv 1 \bmod 2$,

$$N_q(1+\xi\pi^4) = \frac{1}{4}\cdot(1+q)\cdot[(1+6d+d^2)^2 - 16d(1+d)^2] - 6d - d^2$$
$$+\left[\frac{1-d^2(6+d)^2}{2} + 8d(1+d)\right]\sqrt{q}$$
$$= \sqrt{q}^{4g_4}\cdot(-1+2\sqrt{q})^{2h_4} \equiv 1 \bmod 8.$$

Sei im folgenden $t \geqslant 2$ und $\delta \in \mathbb{Z}[\sqrt{d}]$ eine primitive 4. Einheitswurzel mod 2^{t+1} wie in 2.a; sei $\omega \in \mathbb{Z}[(1+\sqrt{q})/2]$ eine primitive 3. Einheitswurzel mod 2^{t+1} wie in 2.c. Dann ist ω eine Erzeugende von U_w/U_w^1, und folglich hat jedes ganze zu 2 prime $\alpha \in K$ eine Darstellung

$$\alpha = \omega^P \cdot \delta^Q \cdot (1+\xi\pi)^A \cdot (1+\xi\pi^3)^B \cdot (1+\pi^3)^C \cdot (1+\xi\pi^4)^D + 2^t\beta \qquad (5)$$

mit P, Q, A, B, C, $D \geqslant 0$ und ganzem $\beta \in K$. Dabei ist P mod 3, Q mod 4, A mod 2^t, B mod 2^{t-1}, C mod 2^{t-1}, und D mod 2^{t-2} eindeutig bestimmt.

In vielen Fällen ist es nun möglich, die Restklasse von α mod 2^t auf Grund der Darstellungen von[2] $N(\alpha)$ durch quadratische Formen zu bestimmen.

THEOREM. *Sei $\alpha \in K$ ganz, prim zu 2, und in der Darstellung (5) gegeben. Dann gilt:*

(i) *Genau dann ist $P \equiv 0 \bmod 3$, wenn $N(\alpha) = X^2 - qY^2$ mit $X, Y \in \mathbb{Z}$; andernfalls ist $4N(\alpha) = X^2 - qY^2$ mit $X, Y \in \mathbb{Z}$, $X \equiv Y \equiv 1 \bmod 2$.*

(ii) *Genau dann ist $A \equiv 0 \bmod 2$, wenn $N(\alpha) = X^2 - 4q^*Y^2$ mit $X, Y \in \mathbb{Z}$; andernfalls ist $N(\alpha) = 4X^2 - q^*Y^2$ mit $X, Y \in \mathbb{Z}$.*

(iii) *Genau dann bestehen die Kongruenzen $A \equiv B \equiv C \equiv 0 \bmod 2^{t-1}$, $D \equiv 0 \bmod 2^{t-2}$ und $P \equiv 0 \bmod 3$, wenn $N(\alpha) = X^2 - 4^t dY^2 = X_1^2 - 4^t q^* Y_1^2 = X_2^2 - 4^t q Y_2^2$ mit $X, X_1, X_2, Y, Y_1, Y_2 \in \mathbb{Z}$, $X \equiv X_1 \equiv 1 \bmod 2^t$ und $X_2 \equiv 1 + 2^t Y_2 \bmod 2^{t+1}$.*

(iv) *Sei $C \equiv 0 \bmod 2^{t-1}$. Genau dann bestehen darüber hinaus auch die Kongruenzen $A \equiv 0 \bmod 2^t$, $B \equiv 0 \bmod 2^{t-1}$ und $D \equiv 0 \bmod 2^{t-2}$, wenn $N(\alpha) = X^2 - 4^t dY^2 = X_1^2 - 4^t q^* Y_1^2$ mit $X, X_1, Y, Y_1 \in \mathbb{Z}$, $X \equiv X_1 \equiv 1 \bmod 2^t$ und $Y \equiv Y_1 \bmod 2$.*

[2] $N(\alpha)$ ist in diesem Abschnitt die Norm von α bzgl. $K/\mathbb{Q}$.

(v) *Sei* $A \equiv 0 \bmod 2^t$. *Genau dann bestehen darüber hinaus auch die Kongruenzen* $P \equiv 0 \bmod 3$, $B \equiv C \equiv 0 \bmod 2^{t-1}$ *und* $D \equiv 0 \bmod 2^{t-2}$, *wenn* $N(\alpha) = X^2 - 4^t dY^2 = X_2^2 - 4^t q Y_2^2$ *mit* $X, X_2, Y, Y_2 \in \mathbb{Z}$, $X \equiv 1 \bmod 2^t$ *und* $X_2 \equiv 1 + 2^t Y_2 \bmod 2^{t+1}$.

Beweis. Sei α in der Darstellung (5) gegeben und

$$\alpha_0 = (1+\xi\pi)^A \cdot (1+\xi\pi^3)^B \cdot (1+\pi^3)^C \cdot (1+\xi\pi^4)^D,$$

also $\alpha = \omega^P \delta^Q \alpha_0 + 2^t\beta$. Dann ist

$$N_d(\alpha_0) = \pm 5^{Ab_1 + Bb_2 + 2Cb_3 + Db_4} \cdot (-1 + 2\sqrt{d})^{2Ac_1 + Bc_2 + 2Cc_3 + 4Dc_4},$$
$$N_{q^*}(\alpha_0) = \sqrt{q^*}^{Ae_1 + 2Be_2 + 2Ce_3 + 2De_4} \cdot (-1 + 2\sqrt{q^*})^{Af_1 + Bf_2 + 4Cf_3 + 4Df_4},$$
$$N_q(\alpha_0) = \pm \sqrt{q}^{2Ag_1 + 4Bg_2 + 2Cg_3 + 4Dg_4} \cdot (-1 + 2\sqrt{q})^{Ah_1 + Bh_2 + 2Ch_3 + 2Dh_4}.$$

Genau dann ist $N_d(\alpha_0) \equiv \pm 1 \bmod 2^t$, wenn

$$\begin{aligned} Ab_1 + Bb_2 + 2Cb_3 + Db_4 &\equiv 0 \bmod 2^{t-2}, \\ 2Ac_1 + Bc_2 + 2Cc_3 + 4Dc_4 &\equiv 0 \bmod 2^{t-1}; \end{aligned} \tag{6_1}$$

genau dann ist $N_{q^*}(\alpha_0) \equiv 1 \bmod 2^t$, wenn

$$\begin{aligned} Ae_1 + 2Be_2 + 2Ce_3 + 2De_4 &\equiv 0 \bmod 2^{t-1}, \\ Af_1 + Bf_2 + 4Cf_3 + 4Df_4 &\equiv 0 \bmod 2^{t-1}; \end{aligned} \tag{6_2}$$

genau dann ist $N_q(\alpha_0) \equiv \pm 1 \bmod 2^t$, wenn

$$\begin{aligned} 2Ag_1 + 4Bg_2 + 2Cg_3 + 4Dg_4 &\equiv 0 \bmod 2^{t-1}, \\ Ah_1 + Bh_2 + 2Ch_3 + 2Dh_4 &\equiv 0 \bmod 2^{t-2}. \end{aligned} \tag{6_3}$$

Die Kongruenzen (6_1), (6_2), (6_3) betrachte ich als homogenes Gleichungssystem modulo 2^{t-1} für A, B, $2C$, $2D$; es hat die Koeffizientenmatrix

$$\mathfrak{A} = \begin{pmatrix} 2b_1 & 2b_2 & 2b_3 & b_4 \\ 2c_1 & c_2 & c_3 & 2c_4 \\ e_1 & 2e_2 & e_3 & e_4 \\ f_1 & f_2 & 2f_3 & 2f_4 \\ 2g_1 & 4g_2 & g_3 & 2g_4 \\ 2h_1 & 2h_2 & 2h_3 & 2h_4 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \bmod 2. \tag{7}$$

$\mathfrak{A}$ hat modulo 2 den Rang 4, also hat das homogene Gleichungssystem modulo 2^{t-1} nur die triviale Lösung. Folglich ist genau dann

$N_d(\alpha_0) \equiv 1 \bmod 2^t$, $N_{q^*}(\alpha_0) \equiv 1 \bmod 2^t$ und $N_q(\alpha_0) \equiv 1 \bmod 2^t$ wenn $A \equiv B \equiv 0 \bmod 2^{t-1}$, $C \equiv D \equiv 0 \bmod 2^{t-2}$.

Wegen $N_q(\alpha) \equiv \omega^{2P} \bmod 2$ und $N_{q^*}(\alpha) \equiv \sqrt{q^*}^A \bmod 2$ folgen (i) und (ii) aus 2.b und c.

Im folgenden sei gemäß [22]

$$\beta = \tfrac{1}{2} \cdot (\beta_0 + \beta_1 \sqrt{q} + \beta_2 \sqrt{d} + \beta_3 \sqrt{q^*}) \tag{8}$$

mit $\beta_j \in \mathbb{Z}$, $\beta_0 \equiv \beta_1 \bmod 2$ und $\beta_2 \equiv \beta_3 \bmod 2$. Wegen (ii) kann ich für den Rest des Beweises $A \equiv 0 \bmod 2$, also $\alpha_0 \equiv 1 \bmod 2$, voraussetzen.

(iii) Wegen (i) kann ich $P \equiv 0 \bmod 3$ annehmen; dann ist $\alpha = \delta^Q \alpha_0 + 2^t \beta$ mit $\alpha_0 \equiv 1 \bmod 2$. Ich bezeichne mit σ_q den erzeugenden Automorphisms für $K/\mathbb{Q}(\sqrt{q})$ und erhalte

$$N_q(\alpha) \equiv N_q(\alpha_0) + 2^t \cdot [\delta^Q \cdot \sigma_q(\beta) + \sigma_q(\delta^Q) \cdot \beta] \bmod 2^{t+1},$$

also wegen $\delta^Q \cdot \sigma_q(\beta) + \sigma_q(\delta^Q) \cdot \beta \equiv 0 \bmod 2$ (unter Benutzung von (8))

$$N_q(\alpha) \equiv N_q(\alpha_0) \bmod 2^{t+1}.$$

Nach 2. ist genau dann $N(\alpha) = X^2 - 4^t dY^2 = X_1^2 - 4^t q^* Y_1^2 = X_2^2 - 4^t q Y_2^2$ mit $X, X_1, X_2, Y, Y_1, Y_2 \in \mathbb{Z}$, $X \equiv X_1 \bmod 2^t$ und $X_2 \equiv 1 + 2^t Y_2 \bmod 2^{t+1}$, wenn $N_d(\alpha) \equiv \pm 1 \bmod 2^t$, $N_{q^*}(\alpha) \equiv \pm 1 \bmod 2^t$ und $N_q(\alpha) \equiv \pm 1 \bmod 2^{t+1}$.

Ist nun $A \equiv B \equiv C \equiv 0 \bmod 2^{t-1}$ und $D \equiv 0 \bmod 2^{t-2}$, so folgt $N_d(\alpha) \equiv \pm N_d(\alpha_0) \equiv \pm 1 \bmod 2^t$, $N_{q^*}(\alpha) \equiv N_{q^*}(\alpha_0) \equiv 1 \bmod 2^t$ und $N_q(\alpha) \equiv N_q(\alpha_0) \equiv \pm 1 \bmod 2^{t+1}$; daher hat $N(\alpha)$ die Darstellungen wie behauptet.

Hat umgekehrt $N(\alpha)$ die angegebenen Darstellungen, so folgt $N_d(\alpha_0) \equiv \pm 1 \bmod 2^t$, $N_{q^*}(\alpha_0) \equiv \pm 1 \bmod 2^t$ und $N_q(\alpha_0) \equiv \pm 1 \bmod 2^{t+1}$, also zunächst $A \equiv B \equiv 0 \bmod 2^{t-1}$, $C \equiv D \equiv 0 \bmod 2^{t-2}$ und

$$N_q(\alpha) \equiv \pm \sqrt{q}^{2Cg_3} \equiv 1 \bmod 2^{t+1},$$

woraus wegen $g_3 \equiv 1 \bmod 2$ auch $C \equiv 0 \bmod 2^{t-1}$ folgt.

(iv) Sei $C \equiv 0 \bmod 2^{t-1}$; σ_d bzw. σ_{q^*} sei der erzeugende Automorphismus für $K/\mathbb{Q}(\sqrt{d})$ bzw. $K/\mathbb{Q}(\sqrt{q^*})$. Aus

$$\alpha = \omega^P \delta^Q \alpha_0 + 2^t \beta \qquad \text{und} \qquad \alpha_0 \equiv 1 \bmod 2$$

folgt

$$N_d(\alpha) \equiv \pm N_d(\alpha_0) + 2^t \cdot (u_0 + v_0 \sqrt{d}) \bmod 2^{t+1},$$
$$N_{q^*}(\alpha) \equiv N_{q^*}(\alpha_0) + 2^t \cdot (u_1 + v_1 \sqrt{q^*}) \bmod 2^{t+1}$$

mit

$$u_0 + v_0\sqrt{d} = \sigma_d(\omega^P\delta^Q)\cdot\beta + \omega^P\delta^Q\cdot\sigma_d(\beta),$$
$$u_1 + v_1\sqrt{q^*} = \sigma_{q^*}(\omega^P\delta^Q)\cdot\beta + \omega^P\delta^Q\cdot\sigma_{q^*}(\beta),$$

und eine leichte Rechnung unter Benutzung von (8) zeigt

$$v_0 \equiv v_1 \bmod 2.$$

Genau dann ist $N_d(\alpha_0)\equiv\pm 1 \bmod 2^t$ und $N_{q^*}(\alpha_0)\equiv 1 \bmod 2^t$, wenn (6_1) und (6_2) erfüllt sind. Wegen $C\equiv 0 \bmod 2^{t-1}$ bilden (6_1) und (6_2) ein homogenes Gleichungssystem modulo 2^{t-1} für A, B und $2D$, dessen Koeffizientenmatrix aus der in (7) stehenden durch Streichen der letzten beiden Zeilen und der drittten Spalte entsteht, also den Rang 3 hat. Daher gilt nach 2.:

Genau dann ist $A\equiv B\equiv 0 \bmod 2^{t-1}$ und $D\equiv 0 \bmod 2^{t-2}$, wenn

$$N(\alpha) = X^2 - 4^t\, dY^2 = X_1^2 - 4^t q^* Y_1^2$$

mit $X\equiv X_1\equiv 1 \bmod 2^t$. Nun ist aber

$$N_d(\alpha)\equiv\pm 5^{Db_4}\cdot(-1+2\sqrt{d})^{Bc_2} + 2^t(u_0+v_0\sqrt{d}) \bmod 2^{t+1},$$
$$N_{q^*}(\alpha)\equiv\sqrt{q^*}^{Ae_1+2De_4}\cdot(-1+2\sqrt{q^*})^{Af_1+Bf_2} + 2^t(u_1+v_1\sqrt{d}) \bmod 2^{t+1}$$

also nach 2.a und b

$$Y\equiv\begin{cases} 1+v_0 \bmod 2 & \text{falls} \quad Bc_2\not\equiv 0 \bmod 2^t,\\ v_0 \bmod 2 & \text{falls} \quad Bc_2\equiv 0 \bmod 2^t,\end{cases}$$

$$Y_1\equiv\begin{cases} 1+v_1 \bmod 2 & \text{falls} \quad Af_1+Bf_2\not\equiv 0 \bmod 2^t,\\ v_1 \bmod 2 & \text{falls} \quad Af_1+Bf_2\equiv 0 \bmod 2^t.\end{cases}$$

Wegen $B\equiv Bc_2\equiv Bf_2 \bmod 2^t$, $A\equiv Af_1 \bmod 2^t$ und $v_0\equiv v_1 \bmod 2$ ist genau dann $Y\equiv Y_1 \bmod 2$, wenn $A\equiv 0 \bmod 2^t$.

(v) Ist $A\equiv 0 \bmod 2^t$, $P\equiv 0 \bmod 3$, $B\equiv C\equiv 0 \bmod 2^{t-1}$ und $D\equiv 0 \bmod 2^{t-2}$, so folgt nach (iii)

$$N(\alpha) = X^2 - 4^t\, dY^2 = X_2^2 - 4^t q Y_2^2 \qquad \text{mit} \quad X, X_2, Y, Y_2\in\mathbb{Z},$$
$$X\equiv 1 \bmod 2^t \qquad \text{und} \qquad X_2\equiv 1+2^tY_2 \bmod 2^{t+1}.$$

Habe nun $N(\alpha)$ die angegebenen Darstellungen durch quadratische Formen; nach 2.a und c, ist dann $N_d(\alpha)\equiv\pm 1 \bmod 2^t$ und $N_q(\alpha)\equiv\pm 1 \bmod 2^{t+1}$. Wegen (ii) is $P\equiv 0 \bmod 3$ und folglich $N_d(\alpha_0)\equiv\pm 1 \bmod 2^t$, $N_q(\alpha_0)\equiv\pm 1 \bmod 2^{t+1}$, woraus insbesondere die Kongruenzen (6_1) und

(6_3) folgen. Wegen $A \equiv 0 \bmod 2^t$ bilden (6_1) und (6_3) ein homogenes Gleichungssystem modulo 2^{t-1} für B, $2C$ und $2D$, dessen Koeffizientenmatrix aus der in (7) stehenden durch Streichen der ersten Spalte und der 3. und 4. Zeile entsteht, also den Rang 3 hat; damit folgt $B \equiv 0 \bmod 2^{t-1}$, $C \equiv D \equiv 0 \bmod 2^{t-2}$ und $N_q(\alpha) \equiv N_q(\alpha_0) \equiv \pm\sqrt{q}^{2Cg_3} \equiv 1 \bmod 2^{t+1}$, also auch $C \equiv 0 \bmod 2^{t-1}$.

4. Schwache Zerlegungsgesetze

Es sei $K = \mathbb{Q}(\sqrt{d}, \sqrt{q})$ mit $d \equiv -1 \bmod 8$, $q \equiv 5 \bmod 8$ und q^* wie in 3. h sei die Klassenzahl von K und h_0 der zu 2 prime Anteil von h, also $h = 2^s h_0$ mit $s \geqslant 0$. Sei $t \geqslant 2$, K_t der Strahlklassenkörper modulo 2^t über K und K_t' die größte in K_t liegende 2-Erweiterung. Zur Kennzeichnung der in K_t bzw. K_t' vollzerlegten Primzahlen werde ich die Hauptideale (α) von K mit $\alpha \equiv 1 \bmod 2^t$ kennzeichnen. Ist $\alpha \in K$ prim zu 2 und in der Darstellung (5) gegeben, so kann ich wegen $N(\delta) \equiv 1 \bmod 2^{t+1}$ den Exponenten Q nicht aus den Normen rekonstruieren. Ich setze daher im folgenden voraus:

$$K \text{ enthalte eine Einheit } \eta \text{ mit } \eta \equiv \sqrt{d} \bmod 2. \qquad (*)$$

Diese Voraussetzung ist im später wichtigen Falle $d = -1$ sicher erfüllt. Hat K die Eigenschaft $(*)$, so ist jedes zu 2 prime Hauptideal von K von der Form (α), wobei α in der Darstellung (5) mit $Q = 0$ gegeben ist. Nun gilt zunächst:

Satz 1. *K erfülle $(*)$, und p sei eine Primzahl mit $(d/p) = (q/p) = 1$. Genau dann ist p vollzerlegt in K_t, wenn $p = X^2 - 4^t dY^2 = X_1^2 - 4^t q^* Y_1^2 = X_2^2 - 4^t q Y_2^2$ mit $X, X_1, X_2, Y, Y_1, Y_2 \in \mathbb{Z}$, $X \equiv X_1 \equiv 1 \bmod 2^t$, $X_2 \equiv 1 + 2^t Y_2 \bmod 2^{t+1}$ und $Y \equiv Y_1 \bmod 2$.*

Beweis. Wegen $(d/p) = (q/p) = 1$ ist p vollzerlegt in K. Nach dem Klassenkörper-Zerlegungsgesetz ist p genau dann vollzerlegt in K_t, wenn p in K einen Primteiler (α) mit $\alpha \equiv 1 \bmod 2^t$ bestizt, und das ist äquivalent zur Existenz eines ganzen $\alpha \in K$ mit $\alpha \equiv 1 \bmod 2^t$ und $N(\alpha) = p$. Nach der eingangs gemachten Bermerkung kann ich o. E. α in der Form (5) mit $Q = 0$ darstellen; die Behauptung des Satzes folgt nun aus dem Theorem, (iii) und (iv).

Satz 1 ist typisch für eine ganze Serie von Resultaten, welche unter verschiedenen Voraussetzungen aus dem Theorem in 2. hergeleitet werden können. Ich beschränke mich im folgenden auf zwei markante Sonderfälle.

SATZ 2. *K erfülle* (∗), *es sei* $q>0$ *und für die Grundeinheit* ε_q *von* $\mathbb{Q}(\sqrt{q})$ *sei* $N(\varepsilon_q)=-1$; *ferner sei* $h\equiv 1 \bmod 2$. *Dann gilt für eine Primzahl p mit* $(d/p)=(q/p)=1$:

Genau dann ist p vollzerlegt in K_t', *wenn* $p^h=X^2-4^t\,dY^2=X_1^2-4^t q^* Y_1^2$ *mit* $X, X_1, Y, Y_1\in\mathbb{Z}$, $X\equiv X_1\equiv 1 \bmod 2^t$ *und* $Y\equiv Y_1 \bmod 2$.

Beweis. Sei $\varepsilon_q^*=\varepsilon_q$ oder $\varepsilon_q^*=\varepsilon_q^3$ je nachdem, ob $\varepsilon_q\equiv 1 \bmod 2$ oder $\varepsilon_q\not\equiv 1 \bmod 2$. Ich setze $\varepsilon_q^*=U+V\sqrt{q}$ mit $U, V\in\mathbb{Z}$; wegen $N(\varepsilon_q^*)=U^2-V^2q=-1$ folgt $U\equiv 2 \bmod 4$ und $V\equiv 1 \bmod 2$, also

$$\pm\varepsilon^*\equiv 2+\sqrt{q}\equiv(1+\xi\pi)^2\cdot(1+\pi^3) \bmod 4.$$

Daher ist jedes zu 2 prime Hauptideal in K von der Form (α), wobei α durch (5) mit $Q=C=0$ gegeben ist.

Wegen $h\equiv 1 \bmod 2$ ist K_t'/K Klassenkörper zur Untergruppe

$$\mathfrak{S}=\{\mathfrak{a}\mid \mathfrak{a}^h=(\alpha) \text{ mit } \alpha\equiv\omega^P \bmod 2^t,\ P\geqslant 0\}$$

der Gruppe der zu 2 primen Ideale von K. Daher ist eine rationale Primzahl p mit $(d/p)=(q/p)=1$ genau dann vollzerlegt in K_t', wenn für einen (und dann für alle) Primteiler $\mathfrak{P}$ von p in K gilt: $\mathfrak{P}\in\mathfrak{S}$, d. h., $p^h=N(\alpha)$ mit $\alpha\equiv\omega^P \bmod 2^t$ für ein $P\geqslant 0$. Schreibt man nun α in der Form (5) mit $Q=C=0$, so folgt die Behauptung aus Aussage (iv) des Theorems.

SATZ 3. *K erfülle* (∗), *es sei* $q^*>0$, ε *die Grundeinheit von* $Q(\sqrt{q^*})$ *und* $\varepsilon\eta$ *ein Quadrat in K. Ferner sei* $h\equiv 1 \bmod 2$ *und p eine Primzahl mit* $(d/p)=(q/p)=1$ *und* $p^h=x^2-qy^2$ *mit* $x, y\in\mathbb{Z}$.

Genau dann ist p vollzerlegt in K_t', *wenn* $p^h=X^2-4^t\,dY^2=X_2^2-4^t q Y_2^2$ *mit* $X, Y, X_2, Y_2\in\mathbb{Z}$, $X\equiv 1 \bmod 2^t$ *und* $X_2\equiv 1+2^t Y_2 \bmod 2^{t+1}$.

Beweis. Ich setze $\varepsilon^*=U+V\sqrt{q^*}$ mit $U, V\in\mathbb{Z}$ und erhalte wegen $U^2-q^*V^2=1$ entweder $U\equiv 1 \bmod 2$, $V\equiv 0 \bmod 4$ oder $U\equiv 2 \bmod 4$, $V\equiv 1 \bmod 2$. Im ersten Falle ist $\varepsilon\equiv 1 \bmod 2$, also $\varepsilon\eta\equiv\delta \bmod 2$ und folglich $\varepsilon\eta$ kein Quadrat in K. Also folgt $\varepsilon\equiv\pm(2+\sqrt{q^*})\equiv\pm\delta(1+\xi\pi)^2 \bmod \mathfrak{w}^3$, und $\sqrt{\varepsilon\eta}$ ist eine Einheit von K mit $\sqrt{\varepsilon\eta}\equiv\delta^Q\cdot(1+\xi\pi) \bmod 2$ für ein geeignetes $Q\geqslant 0$. Daher ist jedes zu 2 prime Hauptideal in K von der Form (α), wobei α in der Darstellung (5) mit $Q=A=0$ gegeben ist. Die Behauptung des Satzes folgt nun wie im Beweis von Satz 3, unter Benutzung der Aussagen (i) und (v) des Theorems.

5. POTENZRESTKRITERIEN FÜR QUADRATISCHE EINHEITEN

Ich gebe in diesem Paragraphen zwei Anwendungen der hergeleiteten schwachen Zerlegungsgesetze auf Potenzrestkriterien für quadratische

Einheiten, und zwar beweise ich eine Verallgemeinerung der von E. Lehmer in [15, Conjecture 4], vermuteten Kriterien sowie ein hinreichendes Kriterium für den 8. Potenzcharakter der Grundeinheit von $Q(\sqrt{q^*})$ für Primzahlen $q^* \equiv 3 \bmod 8$.

KRITERIUM 1. *Sei q eine Primzahl, $q \equiv 5 \bmod 8$, ε die Grundeinheit von $\mathbb{Q}(\sqrt{q})$, und sei h die (ungerade) Klassenzahl von $\mathbb{Q}(\sqrt{q}, \sqrt{-1})$. Sei p eine Primzahl, $p \equiv 1 \bmod 8$, $(q/p) = 1$. Genau dann ist ε biquadratischer Rest modulo p, wenn $p^h = x^2 + 16y^2 = u^2 + 16qv^2$ mit $x, y, u, v \in \mathbb{Z}$ und $y \equiv v \bmod 2$.*

KRITERIUM 2. *Sei q^* eine Primzahl, $q^* \equiv 3 \bmod 8$, ε^* Grundeinheit von $\mathbb{Q}(\sqrt{q^*})$, und sei h die (ungerade) Klassenzahl von $\mathbb{Q}(\sqrt{q^*}, \sqrt{-1})$. Sei p eine Primzahl, $p \equiv 1 \bmod 16$, und habe p^h die Darstellungen $p^h = a^2 - q^*b^2 = x^2 + 64y^2 = u^2 + 256q^*v^2$ mit $a, b, x, y, u, v \in \mathbb{Z}$; dann ist ε^* 8. Potenzrest modulo p.*

Der Beweis dieser Kriterien erfolgt mit Hilfe der Sätze 2 und 3 in 4. Dazu sind aber zunächst eine Reihe arithmetischer Hilfsbetrachtungen anzustellen, welche auch für sich von Interesse sind.

5a. *Hilfssätze*

HILFSSATZ 1. *Sei l eine Primzahl, k ein die l-ten Einheitswurzeln enthaltender algebraischer Zahlkörper, $\mathfrak{l}$ ein Primteiler von l in k und e die Verzweigungsordnung von $\mathfrak{l} \mid l$. Sei $\alpha \in k$ prim zu $\mathfrak{l}$ und kein l-ter Potenzrest modulo $\mathfrak{l}^2$. Dann ist für jedes $n \geqslant 0$ die Erweiterung $k(\sqrt[l^n]{\alpha})/k$ vom Grade l^n, $\mathfrak{l}$ ist vollverzweigt in $k(\sqrt[l^n]{\alpha})$, und $\mathfrak{l}$ geht in der Relativdiskriminante von $k(\sqrt[l^n]{\alpha})/k$ zum Exponenten enl^n auf.*

Beweis. Sei $\alpha_n = \sqrt[l^n]{\alpha}$, $k_n = k(\alpha_n)$ und $\mathfrak{l}_n$ ein Primteiler von $\mathfrak{l}$ in k_n. Ich zeige durch Induktion nach $n \geqslant 0$:

$[k_n : k] = l^n$, $\mathfrak{l}$ ist reinverzweigt in k_n, geht in der Relativdiskriminante von k_n/k zum Exponenten enl^n auf, und α_n ist kein l-ter Potenzrest mod $\mathfrak{l}_n^2$.

Für $n = 0$ ist nichts zu zeigen. Sei die Behauptung für $n \geqslant 0$ bewiesen. Dann ist el^n die Verzweigungsordnung von $\mathfrak{l}_n \mid l$ und $k_{n+1} = k_n(\sqrt[l]{\alpha_n})$; nach [12, T. Ia, §11] ist $[k_{n+1} : k_n] = l$, und $\mathfrak{l}_n$ geht in der Relativdiskriminante $\mathfrak{d}(k_{n+1}/k_n)$ zum Exponenten el^{n+1} auf. Wegen $\mathfrak{d}(k_{n+1}/k) = \mathfrak{N}(\mathfrak{d}(k_{n+1}/k_n)) \cdot \mathfrak{d}(k_n/k)^l$ geht $\mathfrak{l}$ in $\mathfrak{d}(k_{n+1}/k)$ zum Exponenten $el^{n+1} + l \cdot enl^n = e(n+1)\, l^{n+1}$ auf. Ich nehme an, α_{n+1} sei l-ter Potenzrest modulo $\mathfrak{l}_{n+1}^2$ in k_{n+1}, etwa $\alpha_{n+1} \equiv \xi^l \bmod \mathfrak{l}_{n+1}^2$ mit ganzem $\xi \in k_{n+1}$. $(1, \alpha_{n+1}, \ldots, \alpha_{n+1}^{l-1})$ ist eine Basis von k_{n+1}/k_n mit der Diskriminante $d(\alpha_{n+1}) = \pm l^l \alpha_n$, deren $\mathfrak{l}_n$-Anteil mit dem von $\mathfrak{d}(k_{n+1}/k_n)$ übereinstimmt; folglich ist $(1, \alpha_{n+1}, \ldots, \alpha_{n+1}^{l-1})$ eine $\mathfrak{l}_n$-Ganzheitsbasis, und $\xi = \sum_{\nu=0}^{l-1} x_\nu \cdot \alpha_{n+1}^\nu$ mit $\mathfrak{l}_n$-ganzen $x_\nu \in k$. Setzt man $\xi_0 = \sum_{\nu=0}^{l-1} x_\nu^l \alpha_n^\nu \in k_n$, so folgt

$\xi^l \equiv \xi_0 \bmod \mathfrak{l}_{n+1}^2$ wegen $\mathfrak{l}_{n+1}^2 \mid l$, also ist $\alpha_{n+1} = \xi_0 + \lambda$ mit $\lambda \in k_{n+1}$, $\mathfrak{l}_{n+1}^2 \mid \lambda$; daraus folgt $\alpha_n = \xi_0^l + \lambda_0$ mit $\lambda_0 \in k_{n+1}$, $\mathfrak{l}_n \mathfrak{l}_{n+1} \mid \lambda_0$, also $\lambda_0 \in k_n$, $\mathfrak{l}_n^2 \mid \lambda_0$, und α_n ist l-ter Potenzrest modulo $\mathfrak{l}_n^2$, ein Widerspruch!

HILFSSATZ 2. *Sei l eine Primzahl, $n \geqslant 1$ und k_n/k eine zyklische Erweiterung algebraischer Zahlkörper vom Grade l^n. k_{n-1} sei der Zwischenkörper von k_n/k mit $[k_n : k_{n-1}] = l$, $\mathfrak{d}_n$ bzw. $\mathfrak{d}_{n-1}$ sei die Relativdiskriminante von k_n/k bzw. k_{n-1}/k, und $\mathfrak{f}_n$ sei der endliche Bestandteil des Führers von k_n/k. Dann ist*

$$\mathfrak{d}_n = \mathfrak{d}_{n-1} \cdot \mathfrak{f}_n^{l^{n-1}(l-1)}.$$

Beweis. Nach [12, T. I, §9], ist $\mathfrak{d}_n$ das Produkt und $\mathfrak{f}_n$ das kleinste gemeinsame Vielfache der Führer $\mathfrak{f}(\chi)$ der Charaktere χ von k_n/k. Daraus erhält man

$$\mathfrak{d}_n = \mathfrak{d}_{n-1} \cdot \prod \mathfrak{f}(\chi),$$

wobei das Produkt über alle Charaktere der Ordnung l^n zu erstrecken ist. Ist χ_0 ein erzeugender Charakter von k_n/k, so sind genau die $\varphi(l^n) = l^{n-1}(l-1)$ Charaktere χ_0^i mit $0 \leqslant i < l^n$, $l \nmid i$, von der Ordnung l^n, und diese sind alle zu χ_0 konjugiert, haben also denselben Führer, woraus

$$\mathfrak{d}_n = \mathfrak{d}_{n-1} \cdot \mathfrak{f}(\chi_0)^{l^{n-1}(l-1)}$$

folgt. Jeder Charakter χ von k_n/k ist zu einer Potenz von χ_0 konjugiert, also ist $\mathfrak{f}(\chi) \mid \mathfrak{f}(\chi_0)$ und daher $\mathfrak{f}(\chi_0) = \mathfrak{f}_n$.

HILFSSATZ 3. *Sei l eine Primzahl und K/k eine abelsche Erweiterung vom Typ (l, l). Dann hat K/k genau $l+1$ Zwischenkörper $k_1, \ldots, k_{l+1}$ mit $[k_i : k] = l$, und für die Relativdiskriminanten gilt:*

$$\mathfrak{d}(K/k) = \prod_{i=1}^{l+1} \mathfrak{d}(k_i/k)^{l-1}.$$

Beweis. Die l^2 zu K/k gehörigen Charaktere bestehen aus $l+1$ Systemen von je $l-1$ zueinander konjugierten Charakteren der Ordnung l und dem trivialen Charakter. Sei $(\chi_1, \ldots, \chi_{l+1})$ ein Repräsentantensystem paarweise nicht-konjugierter Charaktere der Ordnung l und k_i der zu χ_i gehörige Zwischenkörper von K/k. Die Behauptung folgt nun wieder aus dem Führer-Diskriminantensatz in [12, T. I, §9].

Bemerkung. Die Hilfssätze dieses Abschnittes wurden für algebraische Zahlkörper formuliert; sie gelten jedoch in analoger Weise für endliche

Erweiterungen von $\mathbb{Q}_l$ (für die Führer-Diskriminanten-Relationen im lokalen Fall siehe [2, chap. 11; 19, chap. 4]).

5b. *Beweis von Kriterium* 1

SATZ 4. *Sei* $q \in \mathbb{N}$ *quadratfrei,* $q \equiv 5 \bmod 8$, ε *die Grundeinheit von* $\mathbb{Q}(\sqrt{q})$, $N(\varepsilon) = -1$ *und* $K = \mathbb{Q}(\sqrt{q}, \sqrt{-1})$. *Dann gilt*:

(a) *Die Erweiterung* $K(\sqrt[4]{\varepsilon})/K$ *hat den Führer* 2^2.

(b) *Ist die Klassenzahl von* K *ungerade, so gilt für den 2-Strahlklassenkörper modulo* 2^2 *über* K: $K_2' = K(\sqrt[4]{\varepsilon}, \sqrt[4]{-1})$.

Mit Hilfe von Satz 4 ist Kriterium 1 eine unmittelbare Folgerung aus Satz 2, angewandt auf K mit $t = 2$: ε ist genau dann biquadratischer Rest nach einer Primzahl p mit $(q/p) = (-1/p) = 1$, wenn p in $K(\sqrt[4]{\varepsilon})$ vollzerlegt ist; im Falle $p \equiv 1 \bmod 8$ (und nur in diesem Falle sind ε und die dazu konjugierte Einheit $\bar{\varepsilon} = -\varepsilon^{-1}$ beide biquadratische Reste oder beide nicht) ist das aber äquivalent dazu, daß p in $K(\sqrt[4]{\varepsilon}, \sqrt[4]{-1})$ vollzerlegt ist; und dafür gibt Satz 4 im Falle ungerader Klassenzahl h von K wegen $K_2' = K(\sqrt[4]{\varepsilon}, \sqrt[4]{-1})$ ein notwendiges und hinreichendes Kriterium. Daß h tatsächlich ungerade ist, folgt aus des Klassenzahlproduktformel für K ([13], §26) und der Tatsache, daß die Klassenzahl von $\mathbb{Q}(\sqrt{q})$ ungerade und die von $\mathbb{Q}(\sqrt{-q})$ nicht durch 4 teilbar ist.

Beweis von Satz 4. (a) Sei $k = \mathbb{Q}(\sqrt{q})$, $k_1 = k(\sqrt{\varepsilon})$, $k_1' = k(\sqrt{-q})$, $k_2 = k(\sqrt[4]{\varepsilon})$, $k_2' = k(\sqrt{-\sqrt{\varepsilon}})$, $K_1 = k_1 k_1' = K(\sqrt{\varepsilon})$ und $K_2 = k_2 k_2' = K(\sqrt[4]{\varepsilon})$. In k ist 2 unverzweigt, und ε ist quadratischer Nichtrest modulo 4: wegen $N(\varepsilon) = -1$ sind ε und $-\varepsilon^{-1}$ zueinander konjugiert; wäre $\varepsilon = \xi^2 + 4\alpha$ mit ganzen $\xi, \alpha \in k$, so folgte $-\varepsilon^{-1} = \bar{\xi}^2 + 4\bar{\alpha}$ ($\bar{}$: die Konjugation von $k/\mathbb{Q}$), also $-1 = (\xi\bar{\xi})^2 + 4\beta$ mit $\beta \in k$; aber dann ist $\beta \in \mathbb{Q}$, ein Widerspruch! Somit ist Hilfssatz 1 auf die Erweiterung k_2/k anwendbar; diese ist außerhalb 2 unverzweigt, also folgt

$$\mathfrak{d}(k_1/k) = 2^2 \qquad \text{und} \qquad \mathfrak{d}(k_2/k) = 2^8.$$

k_1' ist zu k_1 konjugiert, daher ist $\mathfrak{d}(k_1'/k) = \mathfrak{d}(k_1/k) = 2^2$, $K = k(\sqrt{-1})$ und -1 ist quadratischer Nichtrest modulo 4 in k (beispielsweise nach §2.c), also ist auch $\mathfrak{d}(K/k) = 2^2$. Hilfssatz 3, angewandt auf K_1/k, liefert

$$\mathfrak{d}(K_1/k) = 2^2 \cdot 2^2 \cdot 2^2 = 2^6.$$

Sei nun $\mathfrak{w}$ der Primteiler von 2 in K; aus $\mathfrak{d}(K_1/k) = \mathfrak{N}(\mathfrak{d}(K_1/K)) \cdot \mathfrak{d}(K/k)^2$ folgt

$$\mathfrak{d}(K_1/K) = \mathfrak{w}^2;$$

ist $\mathfrak{l}_1$ der Primteiler von 2 in k_1, so folgt in gleicher Weise

$$\mathfrak{d}(K_1/k_1) = \mathfrak{l}_1^2.$$

Wegen $\mathfrak{d}(k_2/k) = \mathfrak{N}(\mathfrak{d}(k_2/k_1)) \cdot \mathfrak{d}(k_1/k)^2$ folgt $\mathfrak{d}(k_2/k_1) = \mathfrak{l}_1^4$, und da k_2 und k_2' zueinander konjugiert sind, ist auch $\mathfrak{d}(k_2'/k_1) = \mathfrak{l}_1^4$. Nun wende ich Hilfssatz 3 auf K_2/k_1 an und erhalte

$$\mathfrak{d}(K_2/k_1) = \mathfrak{l}_1^4 \cdot \mathfrak{l}_1^4 \cdot \mathfrak{l}_1^2 = \mathfrak{l}_1^{10}.$$

Bezeichnet $\mathfrak{w}_1$ den Primteiler von 2 in K_1, so folgt aus $\mathfrak{d}(K_2/k_1) = \mathfrak{N}(\mathfrak{d}(K_2/K_1)) \cdot \mathfrak{d}(K_1/k_1)^2$

$$\mathfrak{d}(K_2/K_1) = \mathfrak{w}_1^6$$

und damit

$$\mathfrak{d}(K_2/K) = \mathfrak{N}(\mathfrak{d}(K_2/K_1)) \cdot \mathfrak{d}(K_1/K)^2 = \mathfrak{w}^{10}.$$

Mit Hilfssatz 2 folgt nun für den Führer $\mathfrak{f}$ von K_2/K:

$$\mathfrak{w}^{10} = \mathfrak{w}^2 \cdot \mathfrak{f}^2,$$

also

$$\mathfrak{f} = \mathfrak{w}^4 \cong 2^2.$$

(b) Sei $\mathfrak{w}$ der Primteiler von 2 in K. $\sqrt{-1}$ ist quadratischer Nichtrest modulo $\mathfrak{w}^2$ (nach 3. (5)) also hat nach Hilfssatz 1 und 2 $K(\sqrt[4]{-1})/K$ den Führer $\mathfrak{w}^4 \cong 2^2$. Aus (a) folgt nun, daß $K(\sqrt[4]{\varepsilon}, \sqrt[4]{-1})/K$ den Führer 2^2 besitzt; wegen $[K(\sqrt[4]{\varepsilon}, \sqrt[4]{-1}): K] = 8$ bleibt zu zeigen:

$$[K_2': K] = 8.$$

Da K ungerade Klassenzahl besitzt, ist $[K_2': K]$ der 2-Anteil der Ordnung der primen Restklassengruppe modulo 2^2 modulo der von den globalen Einheiten von K erzeugten Untergruppe. Nach 3. (5) hat jedes ganze zu 2 prime $\alpha \in K$ eine Darstellung

$$\alpha \equiv \omega^P \cdot \sqrt{-1}^Q \cdot (1 + \xi\pi)^A \cdot (1 + \xi\pi^3)^B \cdot (1 + \pi^3)^C \bmod 2^2$$

mit eindeutig bestimmten $P \bmod 3$, $Q \bmod 4$, $A \bmod 4$, $B \bmod 2$ und $C \bmod 2$. Die Einheitengruppe von K wird nach [13, §26] von ε und $\sqrt{-1}$ erzeugt, und nach dem im Beweis von Satz 2 Gezeigten ist

$$\varepsilon \equiv (1 + \xi\pi)^2 \cdot (1 + \pi^3) \bmod 2^2.$$

Somit ist der fragliche Index $(4 \cdot 4 \cdot 2 \cdot 2)/(4 \cdot 2) = 8$, wie behauptet wurde.

5c *Beweis von Kriterium* 2

SATZ 5. *Sei* $q^* \in \mathbb{N}$ *quadratfrei,* $q^* \equiv 3 \bmod 8$, $K = \mathbb{Q}(\sqrt{q^*}, \sqrt{-1})$, ε^* *die Grundeinheit von* $\mathbb{Q}(\sqrt{q^*})$ *und* $\varepsilon_0 \in K$ *mit* $\varepsilon_0^2 = \varepsilon^* \cdot \sqrt{-1}$. *Dann gilt:*

(a) *Die Erweiterung* $K(\sqrt{\varepsilon_0})/K$ *hat den Führer* 2^2, *und* $K(\sqrt[4]{\varepsilon_0})/K$ *hat den Führer* 2^3.

(b) *Ist die Klassenzahl von* K *ungerade, so gilt für die* 2-*Strahlklassenkörper modulo* 2^2 *und* 2^3:

$$K_2' = K(\sqrt[4]{-1}, \sqrt{\varepsilon_0}),$$
$$K_3' = K(\sqrt[8]{-1}, \sqrt[4]{\varepsilon_0}, \sqrt{1-\sqrt{-1}}).$$

Beweis. (a) Sei $\mathfrak{w}$ der Primteiler von 2 in K. Wie im Beweis von Satz 3 erhält man $\varepsilon_0 \equiv \sqrt{-1}^Q \cdot (1+\xi\pi) \bmod \mathfrak{w}^2$, also ist ε_0 quadratischer Nichtrest modulo $\mathfrak{w}^2$, und (was später benötigt wird) $\varepsilon_0^{-1} \cdot \sqrt{-1}$ ist kein Quadrat in K. Nach Hilfssatz 1 gilt für die Relativdiskriminanten $\mathfrak{d}(K(\sqrt{\varepsilon_0})/K) = \mathfrak{w}^4$ und $\mathfrak{d}(K(\sqrt[4]{\varepsilon_0})/K = \mathfrak{w}^{16}$, also hat nach Hilfssatz 2 die Erweiterung $K(\sqrt{\varepsilon_0})/K$ den Führer $\mathfrak{w}^4 \cong 2^2$, und $K(\sqrt[4]{\varepsilon_0})/K$ hat den Führer $(\mathfrak{w}^{16} \cdot \mathfrak{w}^{-4})^{1/2} = \mathfrak{w}^6 \cong 2^3$.

(b) $\sqrt{-1}$ ist quadratischer Nichtrest modulo $\mathfrak{w}^2$ (nach 3. (5)); daraus folgt wie in (a), daß $K(\sqrt[4]{-1})/K$ den Führer 2^2 und $K(\sqrt[8]{-1})/K$ den Führer 2^3 hat; $1-\sqrt{-1}$ ist Primelement für $\mathfrak{w}$ in K, also hat $K(\sqrt{1-\sqrt{-1}})/K$ nach [12, T. Ia, §1] die Relativdiskriminante und damit auch den Führer $\mathfrak{w}^5$. Gemeinsam mit dem in (a) Bewiesenen folgt $K(\sqrt[4]{-1}, \sqrt{\varepsilon_0}) \subset K_2'$ und $K(\sqrt[8]{-1}, \sqrt[4]{\varepsilon_0}, \sqrt{1-\sqrt{-1}}) \subset K_3'$; da $\sqrt{-1}$, ε_0 und $1-\sqrt{-1}$ modulo $K^{\times 2}$ unabhängig sind, folgt $[K(\sqrt[4]{-1}, \sqrt{\varepsilon_0}): K] = 4$ und $[K(\sqrt[8]{-1}, \sqrt[4]{\varepsilon_0}, \sqrt{1-\sqrt{-1}}): K] = 32$; also bleibt zu zeigen:

$$[K_2': K] = 4, \qquad [K_3': K] = 32.$$

Da K ungerade Klassenzahl hat, ist $[K_t': K]$ der 2-Anteil der Ordnung der primen Restklassengruppe modulo 2^t modulo der von den globalen Einheiten von K erzeugten Untergruppe ($t = 2$ oder $t = 3$). Nach 3. (5) hat jedes ganze zu 2 prime $\alpha \in K$ eine Darstellung.

$\alpha \equiv \omega^P \cdot \sqrt{-1}^Q \cdot (1+\xi\pi)^A \cdot (1+\xi\pi^3)^B \cdot (1+\pi^3)^C \cdot (1+\xi\pi^4)^D \bmod 2^t$ mit eindeutig bestimmten $P \bmod 3$, $Q \bmod 4$, $A \bmod 2^t$, $B \bmod 2^{t-1}$, $C \bmod 2^{t-1}$, und $D \bmod 2^{t-2}$. Die Einheitengruppe von K wird nach [13, §26] von ε_0, $\sqrt{-1}$ und einer eventuell (im Falle $q^* = 3$) in K liegenden

dritten Einheitswurzel erzeugt. Wegen $\varepsilon_0 \equiv \sqrt{-1}^Q \cdot (1+\zeta\pi) \bmod 2$ (mit geeignetem Q) ist der fragliche Index

$$\frac{4 \cdot 2^t \cdot 2^{t-1} \cdot 2^{t-1} \cdot 2^{t-2}}{4 \cdot 2^t} = 2^{3t-4},$$

wie behauptet.

Beweis von Kriterium 2. Sei q^* eine Primzahl, $q^* \equiv 3 \bmod 8$, ε^* die Grundeinheit von $\mathbb{Q}(\sqrt{q^*})$ und $K = \mathbb{Q}(\sqrt{q^*}, \sqrt{-1})$. Nach [13, §26] gibt es ein $\varepsilon_0 \in K$ mit $\varepsilon_0^2 = \varepsilon^* \cdot \sqrt{-1}$, und die Klassenzahl h von K ist ungerade, so daß Satz 3 und Satz 5 anwendbar sind.

Sei p eine Primzahl, $p \equiv 1 \bmod 16$, $p = a^2 - q^* b^2$ und $p^h = x^2 + 64y^2 = u^2 + 256q^* v^2$ mit $a, b, x, y, u, v \in \mathbb{Z}$. Dann ist notwendig $x \equiv \pm 1 \bmod 8$, $u \equiv \pm 1 \bmod 8$, und aus Satz 3 folgt:

(a) p ist vollzerlegt in K_2';

(b) Genau dann ist p vollzerlegt in K_3', wenn $u \equiv \pm 1 \bmod 16$, d.h., wenn $p \equiv 1 \bmod 32$.

Sei zunächst $p \equiv 1 \bmod 32$; wegen $\sqrt[4]{\varepsilon_0} \in K_3'$ ist dann ε_0 biquadratischer Rest und $\varepsilon_0^2 = \varepsilon^* \cdot \sqrt{-1}$ 8. Potenzrest modulo p. Da aber auch $\sqrt{-1}$ 8. Potenzrest modulo p ist, folgt: ε^* ist 8. Potenzrest modulo p, was zu zeigen war.

Sei nun $p \equiv 17 \bmod 32$; dann ist p nicht vollzerlegt in K_3', aber wegen (a) und $p \equiv 1 \bmod 16$ ist p vollzerlegt in $K(\sqrt[8]{-1}, \sqrt{\varepsilon_0})$. Wegen $p^h = x^2 + 64y^2$ mit $h \equiv 1 \bmod 2$ ist $p = x_0^2 + 64y_0^2$ mit $x_0, y_0 \in \mathbb{Z}$, also ist 2 ein biquadratischer Rest modulo p (nach [12, T. II, §13]). Nun ist aber $(1-\sqrt{-1})^2 = -2\sqrt{-1}$, und $-\sqrt{-1}$ ist biquadratischer Rest modulo p, also ist $1-\sqrt{-1}$ quadratischer Rest modulo p und daher p vollzerlegt in $K(\sqrt[8]{-1}, \sqrt{\varepsilon_0}, \sqrt{1-\sqrt{-1}})$. Da p in K_3' nicht vollzerlegt ist, ist ε_0 zwar quadratischer, aber kein biquadratischer Rest modulo p. Folglich ist $\varepsilon_0^2 = \varepsilon^* \cdot \sqrt{-1}$ zwar biquadratischer Rest, aber kein 8. Potenzrest modulo p; wegen $p \equiv 17 \bmod 32$ gilt dasselbe für $\sqrt{-1}$, also ist ε^* 8. Potenzrest modulo p, was zu zeigen war

Zusatz bei der Korrektur. Kriterium 1 wurde inzwischen mit anderen Methoden auch von K. Kramer bewiesen [Residue properties of certain quadratic units, *J. Number Theory* **21** (1985), 204–213]. Für einen weiteren Beweis und eine Verschärfung von Kriterium 2 siehe [F. Halter-Koch, Konstruktion von Klassenkörpern und Potenzrestkriterien für quadratische Einheiten, *Manuscripta math.* 1986].

LITERATUR

1. A. AIGNER, Kriterien zum 8. und 16. Potenzcharakter der Reste 2 und -2, *Deutsche Math.* **4** (1939), 44–52.
2. E. ARTIN AND J. TATE, "Class Field Theory," Havard, Cambridge, Mass., 1967.
3. P. BARRUCAND AND H. COHN, Note on primes of type $x^2 + 32y^2$, class number, and residuacity, *J. Reine Angew. Math.* **238** (1969), 67–70.
4. D. BERNARDI, Résidus de puissances, Thèse de 3^e cycle, Publ. Math., d'Orsay, 1979.
5. D. BERNARDI, Résidus de puissances, Sem. Delange-Pisot-Poitou 1977/1978, No. 28.
6. D. BERNARDI, Résidues de puissances et formes quadratiques, *Ann. Inst. Fourier* **30** (1980), 7 – 17.
7. R. EVANS, The octic and biotic character of certain quadratic units, *Utilitas Math.* **25** (1984), 153–157.
8. F. HALTER-KOCH, Kriterien zum 8. Potenzcharakter der Reste 3, 5 und 7, *Math. Nachr.* **44** (1970), 129–144.
9. F. HALTER-KOCH, Einseinheitengruppen und prime Restklassengruppen in quadratischen Zahlkörpern, *J. Number Theory* **4** (1972), 70–77.
10. F. HALTER-KOCH, P. KAPLAN, AND K. S. WILLIAMS, An Artin character and representations of primes by binary quadratic forms II, *Manuscripta Math.* **37** (1982), 357–381.
11. H. HASSE, "Number Theory," Springer, Berlin/New York, 1980.
12. H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, T. I, Ia, und II, Physica-Verlag, Würzburg, 1965.
13. H. HASSE, "Über die Klassenzahl abelscher Zahlkörper," Berlin, 1952.
14. P. KAPLAN AND K. S. WILLIAMS, An Artin character and representations of primes by binary quadratic forms, *Manuscripta Math.* **33** (1981), 339–356.
15. E. LEHMER, On the quartic character of quadratic units, *J. Reine Angew. Math.* **268/269** (1974), 294–301.
16. P. A. LEONARD AND K. S. WILLIAMS, The quadratic and quartic character of certain quadratic units, II, *Rocky Mountain J. Math.* **9** (1979), 683–692.
17. H. v. LIENEN, Primzahlen als 8. Potenzreste, *J. Reine Angew. Math.* **266** (1974), 107–117.
18. P. SATGE, Décomposition des nombres premiers dans des extensions non abéliennes, *Ann. Inst. Fourier* **27** (1977), 1–8.
19. J.-P. SERRE, Local class field theory, *in* "Algebraic Number Theory" (J. W. S. Cassels and A. Fröhlich, Eds.), Academic Press, New York, 1967.
20. A. WESTERN, Some criteria for the residues of eighth and other powers, *Proc. London Math. Soc. (2)* **9** (1911), 244–272.
21. A. L. WHITEMAN, The sixteenth power residue character of 2, *Canad. J. Math.* **6** (1954), 364–376.
22. K. S. WILLIAMS, Integers of biquadratic fields, *Canad. Math. Bull.* **13** (1970), 519–526.